

MMM  
4-29-2005

now US Pat. 6,789,116<sup>2</sup>  
al., filed June 30, 2000, ~~Attorney/Agent Reference Number APPT-001-5~~, and incorporated herein by reference.

## FIELD OF INVENTION

[0008] The present invention relates to computer networks, specifically to the real-time elucidation of packets communicated within a data network, including classification according to protocol and application program.

## BACKGROUND TO THE PRESENT INVENTION

[0009] There has long been a need for network activity monitors. This need has become especially acute, however, given the recent popularity of the Internet and other internets—an “internet” being any plurality of interconnected networks which forms a larger, single network. With the growth of networks used as a collection of clients obtaining services from one or more servers on the network, it is increasingly important to be able to monitor the use of those services and to rate them accordingly. Such objective information, for example, as which services (*i.e.*, application programs) are being used, who is using them, how often they have been accessed, and for how long, is very useful in the maintenance and continued operation of these networks. It is especially important that selected users be able to access a network remotely in order to generate reports on network use in real time. Similarly, a need exists for a real-time network monitor that can provide alarms notifying selected users of problems that may occur with the network or site.

[0010] One prior art monitoring method uses log files. In this method, selected network activities may be analyzed retrospectively by reviewing log files, which are maintained by network servers and gateways. Log file monitors must access this data and analyze (“mine”) its contents to determine statistics about the server or gateway. Several problems exist with this method, however. First, log file information does not provide a map of real-time usage; and secondly, log file mining does not supply complete information. This method relies on logs maintained by numerous network devices and servers, which requires that the information be subjected to refining and correlation. Also, sometimes information is simply not available to any gateway or server in order to make a log file entry.

# METHOD AND APPARATUS FOR MONITORING TRAFFIC IN A NETWORK

## CROSS-REFERENCE TO RELATED APPLICATION

- MM M  
4-29-2005*
- [0001] This invention is a continuation of U.S. Patent Application Serial No. 09/608237 for METHOD AND APPARATUS FOR MONITORING TRAFFIC IN A NETWORK to inventors Dietz, et al., filed June 30, 2000, <sup>now US Pat. 6,651,099</sup> ~~Attorney/Agent Reference Number APPT-001-1~~, the contents of which are incorporated herein by reference
- [0002] This invention claims the benefit of U.S. Provisional Patent Application Serial No.: 60/141,903 for METHOD AND APPARATUS FOR MONITORING TRAFFIC IN A NETWORK to inventors Dietz, et al., filed June 30, 1999, the contents of which are incorporated herein by reference.
- [0003] This application is related to the following U.S. patent applications, each filed concurrently with the present application, and each assigned to the assignee of the present invention:
- [0004] U.S. Patent Application Serial No. 09/609179 for PROCESSING PROTOCOL SPECIFIC INFORMATION IN PACKETS SPECIFIED BY A PROTOCOL DESCRIPTION LANGUAGE, to inventors Koppenhaver, et al., filed June 30, 2000, <sup>now US Pat. 6,665,725</sup> ~~Attorney/Agent Reference Number APPT-001-2~~, and incorporated herein by reference.
- [0005] U.S. Patent Application Serial No. 09/608126 for RE-USING INFORMATION FROM DATA TRANSACTIONS FOR MAINTAINING STATISTICS IN NETWORK MONITORING, to inventors Dietz, et al., filed June 30, 2000, <sup>now US Pat. 6,839,751</sup> ~~Attorney/Agent Reference Number APPT-001-3~~, and incorporated herein by reference.
- [0006] U.S. Patent Application Serial No. 09/608266 for ASSOCIATIVE CACHE STRUCTURE FOR LOOKUPS AND UPDATES OF FLOW RECORDS IN A NETWORK MONITOR, to inventors Sarkissian, et al., filed June 30, 2000, <sup>now US Pat. 6,771,646</sup> ~~Attorney/Agent Reference Number APPT-001-4~~, and incorporated herein by reference.
- [0007] U.S. Patent Application Serial No. 09/608267 for STATE PROCESSOR FOR PATTERN MATCHING IN A NETWORK MONITOR DEVICE, to inventors Sarkissian, et